MULTIRATE STRUCTURES FOR ARBITRARY RATE ERROR CONTROL CODING

Amir S. Avesti-Mehr, Kambiz Nayebi and Shohreh Kasaei

Electrical Engineering Department, Sharif University of Technology
Tehran, Iran, 11365-8639
avestimehr@ee.sharif.edu, knayebi@sharif.edu, skasaei@sharif.edu

ABSTRACT

In this paper, we present the most general form for error control coding using finite field multi-rate filters. This method shows how different types of codes can easily be generated by multi-rate filters and filter banks. In all previous works, codes and syndromes were generated using prefilters. Here we present simple multi-rate structures for encoding and generating syndrome. We show that all kinds of arbitrary rate K/L, circulant linear codes can be generated by these structures. Then we claim that a similar simple structure for syndrome generation in all presented cases exist.

1. INTRODUCTION

As all linear codes constitute a vector space on finite fields, it seems to be a good idea to map message space into the code space using linear systems by circular convolution of the message with a fixed filter, called a generator filter.

In previous works [1, 2], many kinds of structures for generating codes have been discussed. Mathematical concepts of filter bank structures in finite fields have been studied carefully [3, 4, 5, 6, 7, 8, 9]. Recently a filter bank structure using finite field wavelet transforms have been considered [10] to produce double circulant codes with the structure shown in Figure 1. In this paper we generalize and simplify this two-band biorthogonal filter bank structure by eliminating the prefilter $\lambda(n)$ and reducing the two-band structure into a simple upsampler followed by a FIR filter, as shown in Figure 2. We carefully discuss the types of codes that can be generated by this structure and show that this simple structure has all capabilities of previously introduced systems. Then we consider the syndrome generator for codes produced using this method. We also show that the syndrome generator with a similar simple structure exists by proving some relevant theorems, and strong evidences leading to a conjecture.

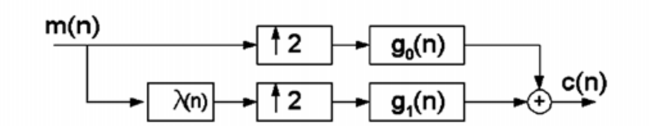

Fig. 1. Code Generator

Arbitrary rate circulant codes with complex structures have been studied previously [11, 12, 13]. Here we also present a simple structure without any prefilters to generate arbitrary rate codes and the corresponding syndromes.

So, while keeping the simplest multirate structure for code and syndrome generation, we still have the capabilities of other structures presented before.

2. GENERAL FILTER BANK STRUCTURE FOR DOUBLE CIRCULANT CODES:

In this section we discuss the encoding of double circulant codes with a rate of $1/2$. For this type of encoding we should map the 2^n n-bit message to a subspace of $2n$-bit codes. Thus the structure in Figure 2 seems to be a good generator for double circulant codes. In this type of structure, filter g is the generator filter and can be selected to produce different codes. The matrix representation of the system can be written as follows.

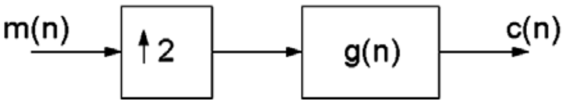

Fig. 2. Code Generator

$$C = G.m \tag{1}$$

where G is defined by

$$\mathbf{G} = \begin{pmatrix} g(0) & g(n-2) & \dots & g(2) \\ g(1) & g(n-1) & \dots & g(3) \\ \vdots & \vdots & \vdots & \vdots \\ g(n-1) & g(n-3) & \dots & g(1) \end{pmatrix}$$

or $G = [2 - circ(g)]^T$.

Now, consider a class of half-rate codes with a partitioned generator matrix given by $G_c = [L^T \; R^T]^T$ in which L and R are two $n \times n$ one-circulant matrices.

Theorem 1. Suppose C is a code over a field F with generator matrix $G_c = [L^T \; R^T]^T$ in which L and R are two $n \times n$ one-circulant matrices. Then the system of Figure 2 constructs the code C_w, an equivalent code to C, if we choose $G_w = PG_c$. Here $P = [p_{i,j}]$ is the matrix

$$p_{\sigma(j),j} = 1 \quad for \quad j = 1, ..., 2n$$

$$p_{i,j} = 0 \quad i \neq \sigma(i) \tag{2}$$

in which σ is a permutation of the set $1, 2, ..., 2n$, defined by :

$$\sigma(i) = 2i - 1 \quad for \quad i = 1, ..., n$$

$$\sigma(i) = 2(i - n) \quad for \quad i = n + 1, ..., 2n \tag{3}$$

Proof: Let C be a (N, M, d) half-rate code generated by G_c. Then, the new code G_w that is obtained by the applying the permutation defined by σ to the code C, has the generator matrix $G_w = PG_c$. It is obvious that the rank of G is equal to n, the rank of G_c. It can also be shown that the matrix G^T is an $n \times 2n$ two-circulant matrix. Thus, if we take g to be equal to the first row of G_w, then diagram of Figure 2 generates the code C_w, an equivalent code to C •

To reach the format of a two band filter-bank, the system in Figure 2 can be divided into two (or more) branches as shown in Figure 3. In each branch, a prefilter can also be added as was previously proposed in [10] and shown in Figure 1 for the two-band case.

It is obvious that diagrams of Figure 2 and Figure 3 are equivalent if we take

$$g = g_0 + g_1 \tag{4}$$

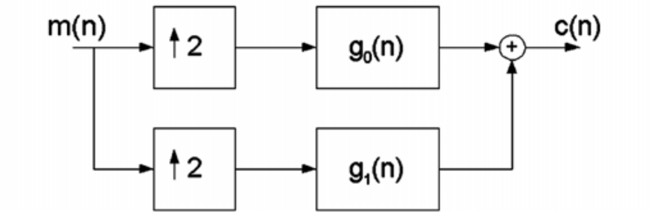

Fig. 3. Two-Band Code Generator

3. SYNDROME GENERATOR STRUCTURE

The important issue for syndrome generator is that if its structure can be as simple as that of the code generator.

Theorem 2. Let $V_1 \subseteq V$ be a subspace of V, the space of rN-bit codes, be r-circulant. Also let $V_2 \perp V_1$ be another subspace of V. Then V_2 is also r-circulant.

Proof: It is sufficient to prove that if $x \in V_2$ then $r-circ(x)$ is also in V_2. If $x \in V_2$ then x is perpendicular to all elements of V_1. Now we show that $r-circ(x)$ is also perpendicular to all elements of V_1, thus $r-circ(x) \in V_2$. Consider $y \in V_1$, as V_1 is r-circulant then $(N-1)r - circ(y)$ $\in V_1$ so x $\perp$(N-1)r-circ(y) which is equivalent to $r-circ(x)$ $\perp y$. Hence V_2 is also r-circulant •

Previous theorem shows that the subspace generated by syndrome generator that is perpendicular to code space is also circulant. Using the results of many computer searches and proofs for special cases, we believe that the following conjecture is true but the complete proof is still an open problem. We use the following conjecture to present a syndrome generator structure for double circulant error correcting codes.

Conjecture 1. Let **V** be a vector space of codes with length $2n$. **W** is a double circulant subspace of **V** that its rank is n and it is generated by a code c and its double circulant shifts. There exists a subspace of **V** named **U** whose rank is equal to n and it is orthogonal to **W**. We state that **U** can also be generated by a code named $\acute{c}$ and its double circulant shifts.

Proof for a Special Case: Suppose that **U** and **W** are disjoint subspaces of **V**. Thus we can write $\mathbf{V} = \mathbf{U} \oplus \mathbf{W}$. Now we define a linear function $T : \mathbf{V} \rightarrow \mathbf{V}, T(x) = x^{2c}$, where $T(x)$ is 2-circulant shift of x. It is obvious that **U** and **W** are invariant under T. As **U** includes a vector whose double circulant shifts form a base for **U**, we know that the minimal polynomial of T over **U** is $x^n - 1$. It is sufficient to prove that the minimal polynomial of T over **W** is also $x^n - 1$. It is obvious that $P(x)$, the minimal polynomial of T over **W**, divides $x^n - 1$. So it is sufficient to prove that degree of $P(x)$ is equal to n. Now suppose that $deg(P) = k$. We have $P(T)(\mathbf{V}) = P(T)(\mathbf{U}) \oplus P(T)(\mathbf{W})$, thus P(T)(**V**)=P(T)(**U**). So dimension of P(T)(**V**) is equal to the dimension of $P(T)$(**U**) that is $n - k$. Now we have **V**=$V_1 \oplus V_2$ such that V_i is a subspace generated by e_i and its double circulant shifts where e_i is a vector that only its ith component is 1 and others are 0. Thus, $P(T)$(**V**)=$P(T)(V_1) \oplus P(T)(V_2)$. As the minimal polynomial of T over both V_1 and V_2 is $x^n - 1$ dimension of $P(T)$(**V**) is equal to $2(n - k)$. So $n - k = 2(n - k)$ then $k = n$ •

Other Evidences: We have verified the truth of the previous conjecture by exhaustive search and verification for codes of length up to 16.

Now suppose that we have generated a double circulant code with the diagram shown in Figure 2. The subspace of code-words named **C** has rank n and it is generated by the vector **g** and its double circulant shifts. Using Conjecture 1 the subspace that is orthogonal to **C** can also be generated by a vector named **h** and its double circulant shifts, so the following structure for syndrome generation always exists.

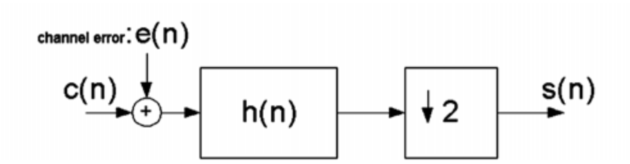

Fig. 4. Syndrome Generator

Example: To generate a linear (12,6,4) code, g can be [000010010101]. Its corresponding h vector will be [110001100101].

4. GENERAL MULTI-RATE STRUCTURE FOR ARBITRARY RATE ERROR CODING:

In this section we generalize the discussions presented in the previous sections to generate codes with the arbitrary rate of K/L using the following structure. Here the code generated can be computed by :

$$C = G.m \tag{5}$$

where G is defined by,

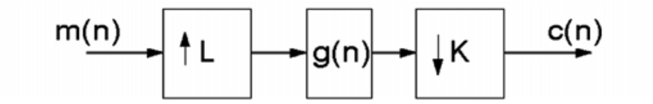

Fig. 5. Generator for arbitrary rate

$$\mathbf{G} = \begin{pmatrix} g(0) & g(((-L))_{nL}) & g(((-2L))_{nL}) & \dots \\ g(K) & g(((K-L))_{nL}) & g(((K-2L))_{nL}) & \dots \\ \vdots & \vdots & \vdots & \vdots \\ g(\alpha) & g(((\alpha-L))_{nL}) & g(((\alpha-2L))_{nL} & \dots \end{pmatrix}$$

where $\alpha = [\frac{n}{K}] * K$.

A theorem similar to Theorem 1 for arbitrary case is as follows.

Theorem 3. Let C be a code over a field F with generator matrix $G_c = [A_1^T \ A_2^T \ \dots \ A_L^T]^T$ in which $A_i s$ are $(\frac{n}{K} \times n)$ K-circulant matrices. Then the diagram of Figure 4 constructs the code C_w, an equivalent code to C, if we choose $G_w = PG_c$ where $P = [p_{i,j}]$ is the matrix

$$p_{\sigma(j),j} = 1 \quad for \quad j = 1, ..., 2n$$

$$p_{i,j} = 0 \quad i \neq \sigma(i) \tag{6}$$

in which σ is a permutation of the set $1, 2, ..., 2n$ defined by :

$$\sigma(i) = (i-1)L + 1 \quad for \quad i = 1, ..., \frac{n}{K}$$

$$\sigma(i) = (i - \frac{n}{K} - 1)L + 2 \quad for \quad i = \frac{n}{K} + 1, ..., 2\frac{n}{K}$$

$$\vdots$$

$$\sigma(i) = (i - (\frac{n}{K})(L-1) - 1)L + L \quad for$$

$$i = \frac{n}{K}(L-1) + 1, ..., L\frac{n}{K} \tag{7}$$

Proof: The proof is similar to the proof of Theorem 1 •

Again this structure can be broken into a K-band structure as shown in Figure 6. As in [10], prefilter can also be added to this multi-band structure. Thus we show that the presented simple multi-rate structure of Figure 5 covers all previously presented systems.

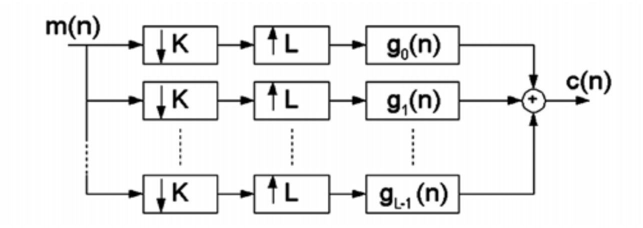

Fig. 6. K-band Generator for arbitrary rate

5. STRUCTURE OF THE SYNDROME GENERATOR FOR ARBITRARY RATE CODES

Here we claim that a syndrome generator with a similar simple structure exist.

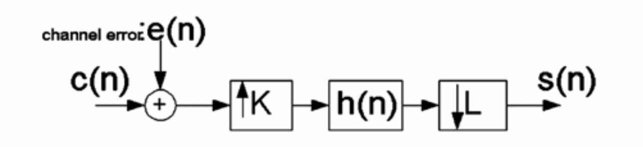

Fig. 7. K-band Generator for arbitrary rate codes

A conjecture similar to Conjecture 1 provides the desired structure for the syndrome generator.
Conjecture 2. Let **V** be a vector space of codes with length $K \times L \times n$. W_1,W_2, . . . and W_{L-1} are L-circulant subspace of **V** that each one has rank equal to $K \times n$ and is generated by a code c and its L-circulant shifts. There exists a subspace of **V** named **U** that its rank is equal to $K \times n$ and it is orthogonal to all W_is. We state that **U** can also be generated by a code named $\acute{c}$ and its L-circulant shifts.

6. CONCLUSION

In this paper, we presented a simple but general multi-rate structure for encoding and syndrome generating for arbitrary rate codes. We stated a conjecture in finite fields whose truth has been partially proved and verified with exhaustive search for small codes (up to length 16). By solving these open problems, one can make sure that such structures can be used for syndrome generation of arbitrary rate circulant codes. In the future, we tend to generalize the basic conditions for existence of these simple structures to generate arbitrary rate codes with a desired minimum distance.

7. REFERENCES

[1] I. F Blake and R. C. Mullin,*The Mathematical Theory of Coding*, Academic press, Inc., 1975.

[2] R. E. Blahut, *Algebric Methods for Signal Procesing and Communications Coding*, New York: Springer-Verlag, 1992.

[3] R. Johannesson and K. S. Zigangirov, *”Fundamentals of Convolutional Coding”*, IEEE press, 1999.

[4] T. Cooklev, A. Nishihara, and M. Sablatash, *Theory of Filter banks over Finite Fields*, in Proc. Asia Paci.c Conf. Circuits Syst., pp. 260 265, Taipei Taiwan, 1994.

[5] K. Nayebi, T. P. Barnwell, and M. J. T. Smith, *Nonuniform Filter banks: a reconstruction and design theory,* IEEE Trans. Signal Proc., vol. 41, June 1993.

[6] F. Fekri, S. W. McLaughlin, R. M. Mersereau, and R. W. Schafer,*Convolutional coding using Finite-Field wavelet transforms*, 2000. in Proc. Thirty-Eighth Annual Allerton Conference.

[7] R. Lidi and H. Niederreiter, *Finite Fields.* Addison-Wesley Publishing Company, 1983.

[8] A. J. Menezes, I. F. Blake, X. Gao, R. C. Mullin, S. A. Vanstone, T. Yaghoobian, *Applications of Finite Fields,* Kluwer Academic Publications, 1993.

[9] G. Caire, R. L. Grossman, and H. V. Poor, *Wavelet transforms associated with finite cyclic groups,* IEEE Trans. on Information Theory, vol. 39, pp. 11571166, July 1993.

[10] F. Fekri, S. W. McLaughlin, R. M. Mersereau, R. W. Schafer,”*Error Control Coding Using Finite Field Wavelet Transforms: Double Circulant Codes*”, submitted to IEEE trans. on Information Theory, December 1999.

[11] P. P. Vaidyanathan, *Multirate Systems and Filter Banks*, Englewood Cliffs, NJ:PrenticeHall, 1993.

[12] P. P. Vaidyanathan,*Multirate digital Filters, Filter banks, polyphase networks, and applications: a tutorial,* Proc. IEEE, vol. 78, pp. 5693, January 1990.

[13] F. Fekri, S. W. McLaughlin, R. M. Mersereau, and R. W. Schafer,*Rate 1/l block codes using Finite Field wavelets; a new family of maximum distance-separable codes and more,* in Proc. Conf. on Information Siences and Systems, Princeton, NJ, March 2000.